IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA,	)	INFORMATION
	)	
Plaintiff,	)	
	)	5:10 CR 00216
v.	)	CASE NO.
	)	Title 18, U.S.C., Sections
MITCHELL L. FROST,	)	1030(a)(5)(A)(i) and
	)	1029(a)(3)
Defendant.	)	JUDGE WELLS

COUNT 1

The United States Attorney charges:

1. At all times material to this Information, defendant, MITCHELL L. FROST, was enrolled as an undergraduate student at the University of Akron. FROST, known by the Internet Relay Chat ("IRC") user name or nickname "FrostAie," used the University of Akron's computer network to access the IRC channels to control other

computers and computer networks via "BotNet" zombies on the Internet, which were located throughout the United States and in other countries.

2. "IRC" is a text-based communications protocol for person-to-person communication or "chat" between computers connected to the Internet. IRC requires one or more "servers" (a computer or software running on a computer, that manages connections between many clients, and relays messages to appropriate recipients) and one or more "clients" (a computer or software running on a computer that is used by a person to chat via IRC). IRC also includes the ability to have private conversations with select clients (users) or public conversations with multiple clients (users). IRC uses channels to determine which users are parties to particular conversations. Private channels may have only two clients, while public channels may have thousands. IRC channels have names that uniquely identify them, and topics which typically describe the topic of discussion on the channel. Users may join a channel and send messages between other users in the same channel. Because Internet connectivity is world-wide, users in a particular channel may be located anywhere in the world. An IRC network is a collection of computers communicating with each other via IRC, and generally includes numerous clients (often up to tens of thousands of clients) and one or several servers.

3. A "bot," derived from the word "robot," generally describes a computer program that performs some predefined function in an automated fashion. An "IRC bot" is a program running as an IRC client that responds autonomously to commands sent to it

by the IRC server. Whereas a typical IRC client application provides information to a human, an IRC bot receives commands, performs numerous functions, and provides information back to the IRC server without human interaction at the client or user level. Bots originally were used to provide interactive access to non-IRC resources, such as a weather bot which would look up weather information for a particular zip code and provide data back to the IRC server. IRC users could then query the weather bot and receive a response based on the weather in the zip code provided. More recently, however, bots have been adapted as a tool for malicious conduct via the Internet. Malicious bots are typically created by individual humans (or groups) who scan the Internet for computers vulnerable to attack or intrusion, use various exploits or malicious computer codes to "hack" into the vulnerable computers, and then install malicious codes (known as malware or bot malware) which enables the hacker to control the hacked computers. Embedded in the malware is an IRC server address (the command and control server), a unique channel name, and any password needed to gain access to that IRC channel. The infected or hacked computer then follows the command it has been given by the hacker to seek out that particular IRC channel, join it, and await commands disseminated by the IRC channel.

4. Typical functions of bot malware installed on an infected computer may include the creation of a "back door" to the infected computer which allows: 1) a malicious controller future access to, and complete control of the infected computer;

2) installation of a keystroke logger which allows the malicious controller to intercept the communications and keystrokes of the user of a bot infected computer; 3) installation of other malware or malicious code on the bot infected computer such as spyware or adware; 4) capture and theft of personal identification and financial information, passwords or web-based e-mail or instant message account log-in information; and 5) capture and theft of software activation codes required to run commercial software.

5. An IRC botnet is an IRC network composed primarily of IRC bots rather than human clients. Most IRC botnets have bots installed on computers rather than human clients. Most IRC botnets have bots installed on computers without the knowledge or consent of the computer's owners, and are generally installed following a remote compromise (i.e. hack), and most malicious IRC bots include codes that enable them to scan for and infect yet additional computers, thereby spreading the botnet to even more computers. Depending upon their intended use, botnets range in size from fewer than one hundred computers to tens of thousands of computers, and will grow and shrink in size as new computers are infected or existing computers are cleaned, shutdown or removed from the Internet. Armed with the range of bot functionality mentioned above, bot controllers or "bot herders" can use the bots within a network in an organized fashion to launch distributed denial of service ("DDoS") attacks, install spam relays for distribution of spam e-mail, install adware for profit generating activities, and engage in high volume thefts of passwords and account login information. A DDoS attack is an

attack designed to flood a computer system or network with an incapacitating volume of traffic in order to overwhelm the victim computer thereby causing it to shut down. The mere threat of a DDoS attack on a victim's site is sometimes used as a tool for extortion of funds from victims.

6. Between in or about July 2006, and on or about March 27, 2007, in the Northern District of Ohio, Eastern Division, and elsewhere, defendant, MITCHELL L. FROST, knowingly caused the transmission of programs, information, codes and commands, and as a result of such conduct, intentionally caused damage to one or more protected computers without authorization.

7. During the time period in question, defendant, MITCHELL L. FROST gained access to other computers and computer networks by various means, including, but not limited to, scanning the Internet for computers and computer networks which were vulnerable to attack or unauthorized intrusion, gaining unauthorized access to and control over such computers, and fraudulently obtaining user name and password login information for users on such computers and networks. FROST then used the compromised computers and computer networks to spread malicious computer codes, commands and information to additional computers and computer networks for the purpose of harvesting and obtaining even more data from those computers, including user names and password login information, credit card numbers, Cvv security codes and other information relating to the account holders (such as names, addresses, social security

numbers and dates of birth), and for the purpose of launching Distributed Denial of Service (DDoS) attacks.

8. During the time period in question, University of Akron computer security administrators determined that defendant, MITCHELL L. FROST, was using the University of Akron computer network to control botnets to gain access to p-store commercial accounts, to spread malware or malicious computer code, to collect credit card information (i.e., account numbers, security codes and account holder personal information), to initiate DDoS attacks and to control other computers without the knowledge or consent of the owners of such computers. Computer logs maintained by the University of Akron network revealed that between on or about August 28, 2006, and on or about March 27, 2007, defendant, MITCHELL L. FROST was involved in programming and distributing malicious code or malware, attacking and compromising remote computer systems, launching DDoS attacks, running botnets, and was engaged in credit card fraud and wire fraud using Western Union. The logs also revealed that defendant, MITCHELL L. FROST attempted to use information collected from his botnet zombies to fraudulently obtain merchandise, services and other things of value.

9. Computer logs maintained by the University of Akron also revealed that during this period of time, defendant, MITCHELL L. FROST discussed ("chatted") with other individuals via IRC concerning various other illegal activities, including the illegal collection and distribution of credit card account information, and engaging in

commercial transactions with the stolen credit card account information to purchase merchandise.

10. Between on or about March 7, 2007, and on or about March 12, 2007, University of Akron computer logs captured data showing defendant, MITCHELL L. FROST initiating Denial of Service (DDoS) attacks on computers connected to the Internet hosting the following Internet websites: www.joinrudy2008.com (2 separate attacks), www.billoreilly.com (5 separate attacks), and www.anncoulter.com (3 separate attacks). These denial of service attacks rendered each website inoperable, at least temporarily, and required intervention and repair by the owners of such sites, and caused damages or losses which exceeded $5,000.00.

11. Defendant, MITCHELL L. FROST, also initiated denial of service attacks against a University of Akron computer server located in the university library on or about March 14, 2007, which caused the entire computer network for the University of Akron to be knocked off-line for approximately 8 ½ hours, thereby preventing all students, faculty and other staff members from accessing the network during this time. Defendant, MITCHELL L. FROST apparently did not intend to attack the University of Akron specifically, but rather intended to attack a gaming server which happened to be housed within the University of Akron network. This attack, however, required the University of Akron to employ diagnostic and remedial measures to restore computer service to the University of Akron community. The denial of service attack defendant,

MITCHELL L. FROST launched against the University of Akron on March 14, 2007, caused losses exceeding $10,000.00 in response, intervention and remediation costs. The University is unable to place a loss amount associated with the loss of the computer network to the tens of thousands of students, faculty and staff members who were unable to access the network during the outage caused by defendant, MITCHELL L. FROST.

12. A federal search warrant covering defendant, MITCHELL L. FROST's dorm room and all computers and other electronic storage media therein was executed by federal agents on or about March 28, 2007. Forensic examination of the computers and other storage media seized pursuant to said search warrant revealed the following items: 136 unauthorized access devices (credit card account numbers, Cvv security codes and card holder Social Security account numbers and other personal identifier information), approximately 2,923 fraudulently obtained computer user login names and passwords for computers and computer networks which defendant, MITCHELL L. FROST was not authorized to access, computer logs showing MITCHELL L. FROST using the IRC bots which automatically scan the Internet looking for vulnerable computers / networks to hack and logs showing MITCHELL L. FROST controlling the Bot network and issuing commands to the Bots which launched DDos attacks against various other computer networks world-wide between June 2006 and March 2007, IRC chat logs of MITCHELL L. FROST and other individuals discussing the establishment and operation of the Bot

network, and approximately 13 copyright motion pictures which had been illegally downloaded from the Internet.

All in violation of Title 18, United States Code, Section 1030(a)(5)(A)(i).

COUNT 2

The United States Attorney further charges:

Between on or about August 28, 2006, and on or about March 27, 2007, in the Northern District of Ohio, Eastern Division, and elsewhere, defendant, MITCHELL L. FROST, did knowingly and with the intent to defraud, possess fifteen or more devices which were counterfeit or unauthorized access devices, such conduct having an effect upon interstate or foreign commerce.

All in violation of Title 18, United States Code, Section 1029(a)(3).

STEVEN M. DETTELBACH
United States Attorney